UNIVERSIDAD VALLE DEL MOMBOY
FACULTAD INGIENIRA
INGENIERIA DE COMPUTACION
SEDE ESTOVACUY

SEGURIDAD INFORMATICA: TECNOLOGIA DE DEFENSA EN PROFUNDIDAD Y PENTESTING

Autor:

Alfonso Andrés Rojo Utrilla

CI: 26.036.511

Tutor:

Dr. Iván Pérez

Febrero, 2020

INDICE GENERAL

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD VALLE DEL MOMBOY
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA INDUSTRIAL
CARVAJAL ESTADO TRUJILLO

ACEPTACIÓN DEL TUTOR

Carvajal, 26 de septiembre de 2019

Ciudadano: Ing. Javier A. Mazzey M.
Director del CIDIFI
Presente.-

Por medio de la presente, hago de su conocimiento, que ante la solicitud realizada por el ciudadano: **Alfonso Andres Rojo Utrilla.** Portador de la C.I.V.-**26.036.511**, acepto el compromiso de Tutorar el desarrollo de su trabajo de investigación titulado: **Seguridad Informática. Tecnologia Defensiva en Profundidad** para optar al titulo universitario en **INGENIERIA EN COMPUTACIÓN**, hasta su presentación y evaluación.

Atentamente,

Prof.(a). Iván Pérez
C.I.Nº 4884756

APROBACIÓN DEL TUTOR

En mi carácter de tutor del trabajo especial de grado, presentado el bachiller: Alfonso Andres Rojo C.I. 26036511, para optar al grado de Ingeniero Industrial cuyo título es: **“Seguridad Informática: Tecnología de Defensa en Profundidad y Penstesting ”** considero que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a la consideración, presentación pública y evaluación por parte del jurado examinador que se designe.

En la ciudad de Valera, a los 10 días del mes de julio de 2019

Dr. Iván Pérez

C.I: V- 4.584.756

TUTOR

UNIVERSIDAD VALLE DEL MOMBOY
FACULTAD INGIENIRA
INGENIERIA DE COMPUTACION
SEDE ESTOVACUY

SEGURIDAD INFORMATICA: TECNOLOGIA DE DEFENSA EN PROFUNDIDAD Y PENTESTING. Autor: Alfonso Andrés Rojo Utrilla. Tutor: Dr. Iván Pérez

RESUMEN

Actualmente la informática y en especial la información es uno de los activos principales de las organizaciones y empresas, existen diferentes tipos de amenazas que atentan contra el buen funcionamiento de estos entes, como los virus, los malware, cibercriminales, spyware y un sinnúmero de amenazas existentes, diariamente se utilizan diferentes equipos que están conectados a internet, que es la mayor fuente de amenazas para la seguridad. En lo relacionado a la seguridad de la información, es relevante destacar que la información en las empresas tiene un valor al igual que cualquier otro recurso, de modo que debe ser protegida. ¿por qué hablar de defensa en profundidad? Claramente si se quiere asegurar la información en cualquier ambiente informático, se debe en cuenta cada aspecto que pueda atentar a la Confidencialidad, Integridad y Disponibilidad de la información, sin pasar por alto alguna etapa en el procesamiento de los datos, ya que con la ausencia de gestión sobre alguno de ellos se deja una puerta abierta ante amenazas que puedan resultar en pérdidas económicas significativas para la organización. Este estudio es de tipo documental, además, según el grado de profundidad es una investigación exploratoria. El objetivo es Describir el modelo de Defensa en Profundidad y el Pentesting como técnicas de seguridad informática.

Palabras Claves: seguridad informática, defensa en profundidad, pruebas de penetración.

UNIVERSIDAD VALLE DEL MOMBOY
FACULTAD INGIENIRA
INGENIERIA DE COMPUTACION
SEDE ESTOVACUY

SEGURIDAD INFORMATICA: TECONOLGIA DE DEFENSA EN PROFUNDIDAD Y PENTESTING. Autor Alfonso Andrés Rojo Utrilla. Tutor: Dr. Iván Pérez

SUMMARY

Currently, information technology and especially information is one of the main assets of organizations and companies, there are different types of threats that threaten the proper functioning of these entities, such as viruses, malware, cybercriminals, spyware and countless threats existing, different computers are used daily that are connected to the internet, which is the biggest source of security threats. With regard to information security, it is relevant to highlight that information in companies has a value just like any other resource, so it must be protected. Why talk about defense in depth? Clearly if you want to secure the information in any computing environment, every aspect that may undermine the Confidentiality, Integrity and Availability of the information must be taken into account, without overlooking any stage in the data processing, since with the absence Management on any of them leaves an open door for threats that may result in significant economic losses for the organization. This study is of documentary type, in addition, according to the degree of depth it is an exploratory investigation. The objective is to describe the Defense in Depth and Pentesting model as computer security techniques.

Keywords: computer security, defense in depth, penetration tests.

NTRODUCCION

Las técnicas tradicionales ya no resultan adecuadas para proteger la información frente a los ciberataques. Además, el creciente uso de las Tecnologías de la Información y Comunicación (TIC´s) se debe a la demanda que existe por el Internet, hay personas que navegan en redes sociales, buscan información, realizan transacciones comerciales en sistemas informáticos entre otros.

Así mismo, conforme avanzan y evolucionan las tecnologías de información, del mismo modo lo hace el entorno de las amenazas cibernéticas, el cual está presente en cada uno de los sistemas informáticos. Aunque se dice que no se puede garantizar la seguridad totalmente, se hace necesario desarrollar mejores métodos de protección frente a dichas amenazas. Con la aparición de nuevos vectores de ataques y amenazas persistentes avanzadas, queda más que claro que se le debe dar un enfoque más moderno a la Seguridad Informática.

En la mayoría de los textos de estudio, relacionados a seguridad de los sistemas informáticos, se lleva a cabo el tratamiento del tema a través del concepto de “Hacking”, es decir actividades que se realizan con el objetivo de encontrar debilidades, vulnerabilidades y potenciales intrusiones sobre los mismos.

La defensa en profundidad de los sistemas de información es una defensa global y dinámica, que coordina varias líneas de defensa que cubren la profundidad del sistema. Los sistemas de información, redes de datos, sistemas operativos y la manipulación no apropiada de la información por parte de los usuarios, han hecho que cada día se presenten más opciones

para los ciberdelincuentes, por ello el aseguramiento en profundidad toma importancia al ser proactivos y evitar pérdida de información en los equipos comprometidos.

En la presente investigación se exponen los factores a tener en cuenta en la defensa en profundidad para proteger la información de la red corporativa, así como la aplicación de pruebas de penetración o pentesting para detectar vulnerabilidades. Además se realiza un diagnostico en cuanto a la situación de la seguridad informática en las Pequeñas y Mediana Empresas en la Ciudad de Valera.

CAPITULO I
EL PROBLEMA

La innovación tecnológica genera nuevas oportunidades pero también nuevos y complejos riesgos, que además no vienen solos sino que cada día están más interrelacionado. Esto es especialmente importante cuando se refiere a la información sensible de las empresas cuyo valor puede ser incalculable y puede determinar el éxito o fracaso de ésta en contra de los beneficios de la competencia.

Los riesgos para la seguridad informática o cyberseguridad están aumentando, tanto en su prevalencia como en su potencial desestabilizador. Los ataques contra las compañías casi se ha duplicado en cinco años y los incidentes que antes se consideraban extraordinarios son cada vez más comunes.

La mejor manera de entender la magnitud del problema que representa los riesgos para la cyberseguridad se evidencia en el Informe Global de riesgos (Global Risks Report), el cual es un documento que viene publicando el Foro Económico Mundial e indica que la tecnología sigue desempeñando una función profunda en la conformación del panorama de riesgos mundiales para individuos, gobiernos y compañías.

Este informe proporciona un análisis riguroso sobre los riesgos a la seguridad global con base en su grado de impacto y probabilidad en un periodo de 10 años, su interrelación, así como las áreas geográficas donde los riesgos globales tienen el mayor potencial sobre la población. Los veintinueve riesgos del informe están clasificados en cinco categorías: económicos, medioambientales, geopolíticos, sociales y tecnológicos.

En este orden de ideas, en el año 2014 fue la primera vez en que dos riesgos tecnológicos aparecieron en el Informe Global de riesgos que publica

el Foro Económico Mundial, ubicándose en quinto lugar la probabilidad de daño a la información crítica de las organizaciones.

Igualmente, en el informe del año 2016, llamado Cuarta Revolución Industrial, se destaca que los ciberataques constituyen la principal amenaza para ocho países entre los que se encuentran Estados Unidos, Japón, Alemania, Suiza y Singapur y aparece entre las cinco principales en otras 27 naciones. El informe apunta que los delitos cibernéticos cuestan a la economía mundial aproximadamente 445.000 millones de dólares

Así mismo, en el informe del año 2017, incluye el incidente masivo de fraude ligado a datos o robo de estos en el quinto lugar, y los ataques cibernéticos a gran escala se posicionaron en el sexto puesto de la lista de los riesgos que es más posible que se haga realidad durante los próximos diez años.

El impacto financiero producto de las violaciones de seguridad cibernética está aumentando y algunos de los mayores costos del 2017 están relacionados con los ataques mediante programas de secuestro cibernético, que representaron el 64 % de todos los correos electrónicos maliciosos. Algunos ejemplos notables incluyeron el ataque WannaCry, que afectó a 300 000 computadoras en 150 países, y Petya, que causó pérdidas trimestrales de USD 300 000 000 a varias compañías afectadas.

Del mismo modo, en 2018 el informe reveló que en términos de probabilidad los ataques cibernéticos ocuparon el tercer lugar y el fraude y robo de datos el cuarto puesto. En este periodo se evidenció otra tendencia creciente es el uso de ataques cibernéticos dirigidos a la infraestructura fundamental y los sectores industriales estratégicos, lo que lleva a temer que, en el peor de los casos, los atacantes podrían desencadenar un colapso de los sistemas que mantienen a las sociedades en funcionamiento.

En el 2018, también vio pruebas continuas de que los ataques cibernéticos plantean riesgos a la infraestructura esencial. En julio, el gobierno de Estados Unidos declaró que los piratas informáticos habían

obtenido acceso a las salas de control de las compañías de servicios públicos estadounidenses. La vulnerabilidad potencial de la infraestructura tecnológica esencial se ha vuelto cada vez más una preocupación de seguridad nacional. Lo ocurrido con Facebook y Cambridge Analytica también explica el aumento de la preocupación global.

Finalmente, en el Informe de Riesgos Mundiales 2019 el fraude y robo de datos masivo se ubicó en el cuarto lugar de riesgo mundial por probabilidad (82%), y los ataques cibernéticos se situaron en el número cinco (80%). Esto mantiene un patrón que se registró en el año 2018, con la consolidación de la posición de los riesgos cibernéticos junto a los riesgos ambientales en el cuadrante de alto impacto y alta probabilidad del panorama de riesgos mundiales.

En este sentido, es necesario entender bien el reto que implica la revolución tecnológica y su impacto en los negocios y las personas, en un mundo cada vez más interconectado, en el que el cambio constante se ha convertido en la nueva normalidad. Es por esto que la principal tarea de la seguridad informática es la de minimizar los riesgos, en este caso provienen de muchas partes, puede ser de la entrada de datos, del medio que transporta la información, del hardware que es usado para transmitir y recibir, los mismos usuarios y hasta por los mismos protocolos que se están implementando, pero siempre la tarea principal es minimizar los riesgos para obtener mejor y mayor seguridad.

En este orden de ideas, la presente investigación se plantea los siguientes objetivos:

OBJETIVO GENERAL

Describir el modelo de Defensa en Profundidad y el Pentesting como técnicas de seguridad informática.

OBJETIVOS ESPECIFICOS

Describir los procedimientos de Seguridad informática, especialmente lo referente a la Defensa en Profundidad.

Caracterizar el pentesting, como método de evaluación integral y detección temprana de fallas de seguridad en los sistemas informáticos.

Diagnosticar la situación actual referente a la Seguridad Informática en las Pequeñas y Medianas Empresas (PyMEs) en la Ciudad de Valera, Estado Trujillo.

Justificación de la Investigación:

Conforme avanzan y evolucionan las Tecnologías de la Información, así mismo lo hace el entorno de las amenazas cibernéticas, el cual está presente en cada uno de los sistemas informáticos. Aunque se dice que no se puede garantizar la seguridad al 100%, se hace necesario desarrollar mejores métodos de protección frente a dichas amenazas. Con la aparición de nuevos vectores de ataques y amenazas persistentes avanzadas, queda más que claro que se le debe dar un enfoque más moderno a la ciberseguridad. Las técnicas tradicionales simplemente ya no resultan adecuadas para proteger la información frente a los ciberataques, en este sentido el presente estudio tiene la siguiente justificación:

Justificación Económica:

Según Kaspersky Lab International, los ataques cibernéticos costaron una media de 1,3 millones de dólares por empresa en 2017 en Norteamérica. Para las PYME, el costo medio de la recuperación asciende a 117.000 dólares. Estas estimaciones incluyen tanto el costo de negocio perdido, las mejoras de software y sistemas y los gastos extra en personal interno y en asesoramiento experto.

Sin embargo, el activo que más está en riesgo es la reputación corporativa. Aquellas empresas que no saben gestionar correctamente su seguridad informática están en peligro de sufrir una caída de reputación. Un informe de Forbes Insights indica que el 46 por ciento de las organizaciones habían sufrido daños en la reputación y en el valor de su marca como resultado de un ataque. Además, de las consecuencias económicas y del daño a su reputación, Según datos de la National Cyber Security Alliance de EE.UU. el 60% de las PYME desaparece dentro de los seis meses siguientes a sufrir un ciberataque.

Así mismo, el informe sobre tendencias de Incidentes e Incumplimientos Cibernéticos que publica cada año la Alianza de Confianza en Línea (OTA, por sus siglas en inglés), con un análisis de las infracciones e incidentes en la Red, estima que se produjeron más de dos millones de ataques informáticos en 2018, aunque estos son los datos registrados y es probable que la cantidad real sea significativamente superior porque no todas las víctimas denuncian. En total, los incidentes cibernéticos del pasado año supusieron un impacto financiero de más de 45.000 millones de dólares, unos 40.000 millones de euros.

Justificación Social:

La ciberseguridad incluye una serie de estrategias, metodologías y tecnologías para resguardar a las organizaciones de las amenazas actuales y es un nuevo punto de partida para lo que vendrá en el futuro, ya que las amenazas tecnológicas que se veían en una película hace algunos años y que parecían de ciencia ficción, hoy están sucediendo, y afectan a todo el mundo sin distinción de país, ideología o raza. En Latinoamérica por ejemplo se ve cada vez más ataques a sistemas financieros e industriales, a infraestructuras críticas y gobiernos, hoy en día nadie está a salvo.

Encuesta Mundial de Seguridad de la Información 2018, revelo que de los principales impactos negativos de un ciberataque para las empresas del

mundo, el daño a la vida humana que representa un 22%, esto se ha evidenciado en los ataques sufridos por las empresas de servicio eléctrico, de transporte, bancarios, entre otros.

John McAffe, dijo: “La tercera Guerra Mundial será una Ciberguerra”, lo cual puede ser cierto, según lo afirmado en la cumbre de la OTAN en 2016:

> “Habiéndose constatado que un ciberataque puede ser tan perjudicial como un ataque convencional, en el campo de la ciberdefensa se han adoptado varias decisiones relevantes, una de ellas es que: El ciberespacio se reconoce como un nuevo dominio de las operaciones, al lado de los de tierra, mar, aire y espacio”.

Justificación Metodológica:

Igualmente, resalta el ámbito metodológico de la investigación que promueve trabajos de investigación en las áreas de la Seguridad Informática, que contribuyan a ampliar el repositorio de Investigaciones dirigidas a un tema de tanta relevancia, estableciendo la necesidad e importancia de adoptar medidas de seguridad apropiadas, lo que le permitirá a las organizaciones contar con un factor diferenciador donde se promueve la seguridad como un pilar fundamental en el quehacer diario que se encuentra en continuo mejoramiento y evolución.

Delimitación

Delimitación espacial:

La presente investigación se desarrollara como requisito para optar al título de Ingeniero en Computación, en la Universidad Valle del Momboy, Sede Estovacuy, Carvajal Estado Trujillo. Venezuela.

Delimitación temporal: Esta investigación fue realizada desde agosto del 2019 hasta febrero del 2020.

CAPITULO II
MARCO TEORICO

Antecedentes de la Investigación

En el año 2015, Torres Douglas, realizo una investigación titulada "Ciberseguridad y Ciberdefensa en Venezuela: Un Enfoque desde los Sistemas Suaves". Esta investigación presenta la situación problema derivada de la utilización de Tecnologías de Información y Comunicación (TIC) y su impacto en la seguridad de la información en Venezuela. Ataques e incidentes cibernéticos sobre Estados, organizaciones y ciudadanos son frecuentes y pueden ser orientados hacia instalaciones de infraestructura crítica de la nación.

La situación problema se sustenta teóricamente desde el paradigma sistémico, donde se aborda la realidad que se estudia, como si fuese un sistema. El uso de Internet por los sectores de la sociedad venezolana, la interacción a través de las telecomunicaciones y de los sistemas de información, deriva en exposición a amenazas cibernéticas. La Metodología de los Sistemas Suaves (MSS) se empleó para el tránsito entre la realidad observada y el mundo de sistemas, donde emerge un Modelo Estratégico de Seguridad y Defensa Cibernética (MESDCI), propuesto como un componente de la estrategia de seguridad, defensa y desarrollo integral, promoviendo el ámbito cibernético como nueva dimensión en el entorno operativo de la República Bolivariana de Venezuela.

La investigación considera que la seguridad y defensa cibernética es un asunto de la sociedad y del Estado, por tanto es seguridad de la Nación. Este estudio fue de utilidad para la presente investigación ya que expone ampliamente las amenazas cibernéticas precisando la importancia de la seguridad informática.

También en el año 2019 Noguera Aaron desarrollo un Trabajo Especial de Grado en la Universidad Central de Venezuela titulado “Implementación de un sistema de detección de Intrusos para Venezolana del Vidrio”. El objetivo principal de este trabajo fue implantar un Sistema de Detección de Intrusos (IDS) en la empresa Venezolana del Vidrio C.A., con el fin de conseguir este objetivo se realizaron diversos análisis a la plataforma tecnológica ya implementada, se llevó a cabo un estudio de la situación actual con la finalidad de definir el mejor escenario a nivel técnico, para llevar a cabo la implantación y puesta en marcha de la solución tecnológica que permitirá ampliar las capacidades de la empresa en cuanto a ciberseguridad se refiere, cumpliendo con la premisa de utilizar una solución basada en software libre con el fin de hacer usos de todas sus bondades.

Durante el levantamiento de información se tomaron en cuenta los aspectos concernientes a la seguridad de la red, ya implantada, proveedores de servicio, dispositivos, software, y accesos a la red empresarial desde localidades externas con las medidas de seguridad y protocolos establecidos para el resguardo de la información. El diseño e implantación se logró de forma satisfactoria, dando así una herramienta que contribuye, con el resguardo de la información de la empresa.

Este Trabajo de Grado sirvió de aporte a la investigación en comento pues trata el tema de ciberseguridad de la red empresarial desde los aspectos de los dispositivos, software proveedores de servicios, entre otros que también son temas tratados y expuestos en esta indagación.

Por último se cita un trabajo realizado por Antonio Inoguchi y Erika Macha en el año 2016, en la Universidad San Ignacio de Loyola de lima Perú. Dicha investigación tuvo como finalidad ayudar a las PYMES del Perú a tomar conciencia en la protección de su data informática y sistemas informáticos, siendo esto fundamental y vital para que las pymes funcionen correctamente y alcance sus. El objetivo propuesto fue obtener un nivel considerable de seguridad para las pymes.

El trabajo de investigación fue valido para la investigación en desarrollo pues habla de los motivos de una fácil intromisión a la información en una red privada, la importancia de plasmar criterios de seguridad de la información para mantener una red privada segura.

Introducción a la Seguridad Informática

Según Aguilera (2011), se puede definir a la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad. Actualmente la informática está siendo inundada por toda la información posible, pero la información por sí sola sigue siendo un universo más grande y en muchos casos más compleja de manejar, ya que los procesos en muchos casos no son tan visibles para los involucrados.

La principal tarea de la seguridad informática es la de minimizar los riesgos, en este caso provienen de muchas partes, puede ser de la entrada de datos, del medio que transporta la información, del hardware que es usado para transmitir y recibir, los mismos usuarios y hasta por los mismos protocolos que se están implementando, pero siempre la tarea principal es minimizar los riesgos para obtener mejor y mayor seguridad.

Lo que debe contemplar la seguridad se puede clasificar en tres partes como son los siguientes:

- Los usuarios
- La información
- La infraestructura

Los usuarios son considerados como el eslabón más débil de la cadena, ya que a las personas es imposible de controlar, un usuario puede un día cometer un error y olvidar algo o tener un accidente y este suceso puede echar a perder el trabajo de mucho tiempo, en muchos casos el

sistema y la información deben de protegerse del mismo usuario. La información se considera como el oro de la seguridad informática ya que es lo que se desea proteger y lo que tiene que estar a salvo, en otras palabras, se le dice que es el principal activo.

Por último, está la infraestructura éste puede ser uno de los medios más controlados, pero eso no implica que sea el que corre menos riesgos, siempre dependerá de los procesos que se manejan. Se deben de considerar problemas complejos, como los de un acceso no permitido, robo de identidad, hasta los daños más comunes, por ejemplo, robo del equipo, inundaciones, incendios o cualquier otro desastre natural que puede tener el material físico del sistema de la organización.

Mecanismos preventivos en seguridad informática

La definición de los mecanismos preventivos, consiste en una serie de revisiones periódicas, algunos cambios o mejoras de diferentes aspectos que pueden ser de hardware, software o de cualquier elemento involucrado en los sistemas y procesos, por eso es que las revisiones dependen de los procesos de la empresa y cada una tiene sus propios procesos. Los mecanismos preventivos en realidad son a largo plazo y por esta razón son considerados por la mayoría como una pérdida de tiempo y dinero.

La mayoría de los ataques informáticos se pueden evitar o por lo menos disminuir el impacto, si se hiciera utilizando mecanismos preventivos, deficiencia de sistemas y otros problemas podrían encontrarse, evitarse y resolverse gracias a un buen trabajo durante esta etapa. La Barrera más fuerte a la que se enfrenta una empresa al querer aplicar los mecanismos preventivos, es la aceptación y el compromiso de todos los involucrados, hacer entender que no es una carga, es parte de los procesos y de lo que se debe hacer bien en la organización.

Mecanismos correctivos en seguridad informática

Los mecanismos correctivos tienen una gran diferencia en tiempo con los mecanismos preventivos, estos se aplican cuando, después de que algo sucedió y la función principal es corregir las consecuencias. Entre las características que tienen los mecanismos correctivos normalmente son muy caros, esto se debe a que el problema ya se lo tiene encima y no se puede tenerlo durante mucho tiempo, así que, contratar expertos para resolver el problema o el tiempo que le dedicara el equipo de trabajo siempre va a costar mucho, en un porcentaje muy alto se acaban pagando servicios de solución a otras empresas, adquiriendo soluciones o comprando software y parches de actualización que logran resolver el problema.

Otra característica de los mecanismos correctivos es que el tiempo es limitado, así que el tiempo se vuelve algo muy apreciado en estos casos, pero también es muy escaso. Probablemente la empresa o la persona puede poder obtener dinero, pero tiempo es casi imposible.

Mecanismos de detección en seguridad informática

Los mecanismos de detección son los más complejos y son en los que se necesita tener alto grado de conocimientos técnicos dependiendo de la materia que se aborde, por ejemplo, seguridad de plataformas en línea, en específico de un tipo de bases de datos o tecnología como Wordpress, esto depende del sistema, aplicación o el ecosistema que tenga funcionando.

Los mecanismos de detección parten de que se tiene la idea de que un atacante es capaz de violar la seguridad y puede haber realizado una intrusión total o parcial a un determinado recurso. Siempre que se trabaja en los mecanismos de detección se tiene la premisa en mente, se debe de trabajar como si lo que se fuera a encontrar es lo peor y se debe estar preparados para la peor de las situaciones posibles**.**

Los tres pilares de la seguridad

Los datos son valores, números, medidas, textos, documentos en bruto, la información es el valor de esos datos, es lo que aporta conocimiento. Los manuales de procedimientos, los datos de los empleados, de los proveedores y clientes de la empresa, la base de datos de facturación son datos estructurados de tal forma que se convierten en información, que aportan valor como compañía.

Los pilares de la seguridad de la información se fundamentan en esa necesidad que todos tienen de obtener la información, de su importancia, integridad y disponibilidad para sacarle el máximo rendimiento con el mínimo riesgo. Los principales pilares de la seguridad de la información son:

- Confidencialidad: La confidencialidad consiste en asegurar que sólo el personal autorizado accede a la información que le corresponde, de este modo cada sistema automático o individuo solo podrá usar los recursos que necesita para ejercer sus tareas, para garantizar la confidencialidad se recurre principalmente a tres recursos:
  - ✓ Autenticación de usuarios: Sirve para identificar qué quién accede a la información es quien dice ser.
  - ✓ Gestión de privilegios: Para los usuarios que acceden a un sistema puedan operar sólo con la información para la que se les ha autorizada y sólo en la forma que se les autorice, por ejemplo, gestionando permisos de lectura o escritura en función del usuario.
  - ✓ Cifrado de información: Según Costas Santos (2011), el cifrado también denominado encriptación, evita que ésta sea accesible a quién no está autorizado, para ello se transforma la información de forma inteligible a una no legible y es aplicable tanto a la información que esté autorizado para ello como para la que no lo está, sólo mediante un sistema de contraseñas puede extraerse la información

de forma inteligible y es aplicable tanto a la información que está siendo transmitida como a la almacenada.

Los principios de confidencialidad no solo deben aplicarse para proteger la información sino todos aquellos datos e información de los que sea responsables. La información puede tener carácter confidencial no solo por ser de alto valor para la organización, sino por ejemplo porque puede estar amparada por legislación de protección de datos de carácter personal, un ejemplo de violación de la confidencialidad son las filtraciones sufridas por entidades bancarias, grandes empresas y gobiernos para exponer públicamente algunas de sus actividades. Los principios de integridad son:

- La integridad: Es el segundo pilar de la seguridad, consiste en asegurarse de que la información no se pierde ni se ve comprometida voluntaria e involuntariamente, el hecho de trabajar con información errónea puede ser tan nocivo para las actividades como perder la información, de hecho, si la manipulación de la información es lo suficientemente sutil puede causar que se arrastre una cadena de errores acumulativos y que sucesivamente se tome decisiones equivocadas. Para garantizar la integridad de la información se debe considerar lo siguiente:

  - ✓ Monitorear el tráfico de red para descubrir posibles intrusiones.
  - ✓ Auditar los sistemas para implementar políticas de auditorías que registre quien hace que, cuando y con qué información.
  - ✓ Implementar sistemas de control de cambios, algo tan sencillo como por ejemplo comprobar los resúmenes de los archivos de información almacenados en sistema para comprobar si cambian o no.
  - ✓ Como otro recurso se tiene las copias de seguridad, que en caso de no conseguir impedir que se manipule o pierda la información permitan recuperarla en su estado anterior.

- Disponibilidad: Para poder considerar que se dispone de una seguridad mínima en lo que a la información respecta, se tiene a la disponibilidad, de nada sirve que solo tanto la información como los servicios estén el usuario acceda a la información y que sea incorruptible, si el acceso a la misma es tedioso o imposible, la información para resultar útil y valiosa debe estar disponible para quien la necesita, se debe implementar las medidas necesarias para que estén disponibles, por ejemplo que la dirección de correo electrónico sea utilizada para lanzar campañas de spam y en consecuencia añadida a listas negras, impidiendo que ninguno de los destinarios de los emails legítimos los reciba.

  La información y sistemas son seguros si sólo accede a la información y recursos quién debe, sí se puede detectar y recuperar de manipulaciones voluntarias o accidentales de la información y si se puede garantizar un nivel de servicio y acceso a la información aceptable según las necesidades.

Principales tendencias de la seguridad informática

En el 2017, varias empresas se vieron afectadas por ciertos virus que irrumpieron en sus sistemas de seguridad, logrando vulnerar la infraestructura de estas corporaciones y generando pánico en el resto de empresas. Entre las más afectadas estuvo la compañía Telefónica, ya que varios centenares de ordenadores de su sede central en Madrid se vieron infectados por un virus malicioso, de tipo ransomware, que bloquea los equipos y solicita un rescate para desbloquearlos.

El Terrible WannaCry

Un ataque masivo de ransomware llamado WannaCry afectó a empresas y particulares de todo el mundo, incluyendo grandes corporaciones y organismos públicos. El ataque golpeó seriamente al Servicio de Salud Británico, a la multinacional francesa Renault, al sistema bancario ruso y al

grupo de mensajería estadounidense FedEx, así como al servicio de ferrocarriles alemán y a universidades en Grecia e Italia. Funcionarios estadounidenses han relacionado la autoría del ataque con el gobierno norcoreano. En este ataque se hizo uso de una vulnerabilidad en un protocolo privativo de Windows que afectaba específicamente a este sistema operativo

El Petya

Aproximadamente un mes después de WannaCry, otra ola de ataques de ransomware aprovechó las vulnerabilidades de Windows expuestas por Shadow Brokers y alcanzó objetivos de todo el mundo. Este malware, conocido como Petya, NotPetya y otros nombres similares, era más avanzado que WannaCry pero aún tenía varios defectos, como un sistema de pago ineficaz.

Aunque infectó redes de múltiples países, los investigadores sospechan que el ransomware en realidad tenía el objetivo de enmascarar un ciberataque dirigido contra instituciones ucranianas. El ransomware afectó

especialmente a la infraestructura de este país, incluyendo a compañías eléctricas, aeropuertos, transporte público y el banco central y ha sido el último de una serie de ataques cibernéticos contra este estado.

Muchas de estas compañías afectadas decidieron tomar las medidas necesarias para evitar este tipo de ataques que no solo afecta la seguridad de la información sino que además atenta contra la reputación de la organización. Dentro de las principales tendencias de seguridad informática se pueden citar:

1. Solución en la Nube

La nube, como arma principal de las empresas, representa una opción confiable y eficaz al momento de implementarla como mecanismo de seguridad. Cuenta con una arquitectura fuerte al mismo tiempo que su diseño permite realizar operaciones seguras. Muchas empresas recurren a este sistema o solución, logrando minimizar el riesgo de ataques, debido a que las configuraciones son realizadas por el mismo proveedor del servicio

2. Arquitectura Fuerte

que evite la intrusión de posibles atacantes. Deben considerarse todos los aspectos que puedan sufrir algún tipo de vulneración y evitarlos en la medida de lo posible.

3. Diseño del Sistema

En cuanto al diseño, la tendencia está en desarrollar un sistema que asegure la solución como un todo. Cada elemento debe estar protegido por separado, y de forma general, el diseño debe prestar especial atención en los datos. Este tipo de infraestructuras permite que el diseño esté compuesto por componentes que están asegurados por separado, como por ejemplo los servidores, la red, entre otros.

4. Operaciones Efectivas

Este término va asociado a esas operaciones que tienen que ver directamente con el sistema, es decir, las acciones que se efectúan y que interaccionan con el mismo. Un ejemplo sería el momento en que se da de alta a un usuario en el sistema o cuando se realiza la configuración de algún servicio, todas estas acciones deben llevarse a cabo de forma segura.

5. Aplicar las mejores practicas

En materia de seguridad, es importante tener un referente de “mejores prácticas” ya que esto facilita las acciones que se realizan en base a cómo deben hacerse las cosas de forma correcta. Cuando tenemos casos en donde conocemos la mejor manera en que pueden realizarse las cosas, tenemos claro hacia dónde puede dirigirse determinada acción. Es fundamental tener una visión que establezca las mejores prácticas en todos los escenarios.

6. Administrar los Riesgos

No todas las empresas son iguales y por ello no todos los riesgos lo son. Es importante tener un referente a la hora de aplicar la administración de riesgos que tome en cuenta el tamaño de la organización, el grado de exposición de riesgos, el tipo de negocio que se desarrolla, tipo de información que se maneja y su importancia, entre otros aspectos. Manejar una amplia gama de posibilidades de riesgos es necesario para saber hasta qué punto quiero proteger mis sistemas y los datos a los que les doy mayor prioridad.

7. Gran Infraestructura

La nueva tendencia en cuanto a seguridad informática es tener una infraestructura robusta y potente que juegue con la optimización de todos los aspectos antes mencionados. Arquitectura sólida, diseño integral de protección, efectividad en las operaciones, aplicar mejores prácticas y saber

administrar los riesgos, además de trabajar con soluciones en la nube que minimicen cualquier riesgo. Finalmente, se puede decir que la seguridad informática depende tanto de las empresas como de los proveedores de los servicios y soluciones que se encargan de mitigar los riesgos.

Defensa en Profundidad

El término defensa en profundidad, también conocido como defensa elástica, se refiere originalmente a una estrategia de defensa militar que consistía en colocar varias líneas defensivas consecutivas en lugar de colocar una línea única muy fuerte. Una de las ventajas de esta estrategia es que el empuje inicial se va perdiendo al tener que superar las distintas barreras. Además la estrategia puede conseguir que la fuerza atacante se disperse, debilitándola por tanto y pudiendo posteriormente el defensor reorganizarse para atacar el punto más debilitado. (Portantier, 2012).

Al igual que un campo de batalla, las infraestructuras de tecnología son una compleja formación de elementos que en conjunto albergan uno de los activos más valiosos para las empresas: los datos. Se puede visualizar esta infraestructura como una serie de capas donde los datos ocupan el último nivel, precedidos de contenedores como lo son las localidades físicas, el perímetro, la red, los servidores y las aplicaciones.

De esta forma, cada capa de nuestra infraestructura representa una barrera para el atacante en su camino hacia el objetivo final de acceder a los datos confidenciales, de manera que si falla cualquiera de los controles en una capa haya defensas adicionales que contengan la amenaza y minimicen las probabilidades de una brecha.

Defensa en profundidad en seguridad informática

La defensa en profundidad también conocido como (Defense in Depth) se trata de un modelo que pretende aplicar controles en seguridad para proteger los datos en diferentes capas.

El concepto de defensa en profundidad se basa en la premisa de que todo componente de un sistema puede ser vulnerado, y por tanto no se debe delegar la seguridad de un sistema en un único método o componente de protección. De esta forma propone el uso de distintas técnicas que permitan, al menos, duplicar los elementos de protección para limitar los daños en caso de una intrusión en la primera línea de defensa o componente más expuesto.

Claramente, si se quiere asegurar la información en cualquier ambiente informático, hay que tener en cuenta cada aspecto que pueda atentar a la Confidencialidad, Integridad y Disponibilidad de la información, sin pasar por alto alguna etapa en el procesamiento de los datos, ya que con la ausencia de gestión sobre alguno de ellos se deja una puerta abierta ante amenazas que puedan resultar en pérdidas económicas significativas para la organización.

El término de defensa en profundidad obedece a seis grandes principios generales. Cada uno de estos principios puede existir de forma individual, pero la profundidad de la defensa la proporciona la combinación de éstos. A continuación, se detalla cada uno:

Tabla Nª 1: Principios Generales de la defensa en Profundidad

TITULO	NATURALEZA
Coordinación	La defensa debe ser dinámica, lo que significa que el sistema de información dispone de una política de seguridad que identifica: a) una capacidad de reacción b) una planificación de las acciones c) una escala de gravedad.
Demostración	La defensa debe ser demostrada, lo que significa que: a) se califica a la defensa b) existe una estrategia de homologación c) la homologación acompaña al ciclo de vida del sistema de información.

Dinamismo	La defensa debe ser dinámica, lo que significa que el sistema de información dispone de una política de seguridad que identifica: a) una capacidad de reacción b) una planificación de las acciones c) una escala de gravedad.
Exhaustividad	La defensa debe ser completa, lo que significa que: a) los bienes que deben protegerse se protegen en función de su criticidad b) que cada uno de ellos está protegido, como mínimo, por tres líneas de defensa c) se formaliza la difusión de la experiencia adquirida.
Globalidad	La defensa debe ser global, lo que significa que engloba todas las dimensiones del sistema de información: a) aspectos organizacionales b) aspectos técnicos c) aspectos de implementación.
Suficiencia	La defensa debe ser suficiente, lo que significa que cada medio de protección (organizacional o técnico) debe contar con: a) una protección propia b) un medio de detección c) procedimientos de reacción.

Fuente: La defensa en profundidad aplicada a los sistemas de información (Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information, 2004).

De acuerdo a Corletti (2017), la defensa en profundidad permite aislar y/o dividir en capas la infraestructura de red con el fin de proporcionar mayor dificultad de acceso no autorizado a la información, a través de los recursos que la transporta y almacena. A continuación se presentan algunos de los factores a tener en cuenta en la defensa en profundidad:

- Firewalls. Representan un mecanismo de defensa inicial hacia toda la red. Las reglas que se apliquen en ellos deben ser muy restrictivas y establecerse por host y servicio.

- Antivirus. Se deben instalar tanto en servidores como equipos clientes, para tareas específicas, como detectores de virus en archivos, herramientas de análisis de contenido y detectores de carga y descarga de datos.

- Redes privadas virtuales. Proporcionan protección a la red ante usuarios remotos, debe requerir autenticación y utilizar tecnologías para suministrar conectividad a los recursos, con sus respectivas reglas de control de acceso.

- Segmentación. Dividir la red para separar el tráfico hacia Internet e Intranet.

- Contraseñas complejas para usuarios. Establecer políticas para establecimiento de contraseñas de cuentas administrativas, usuarios estándar y usuarios remotos.

- Sistemas de administración. Asegurar físicamente las consolas administrativas, equipos de trabajo de administración que controlan los servidores y dispositivos de la red.

- Bitácoras. Se debe configurar el almacenamiento de logs sobre equipos claves, y deben ser revisados periódicamente para detectar actividades sospechosas o anómalas relacionadas con su funcionamiento, mantenimiento y seguridad de los sistemas.

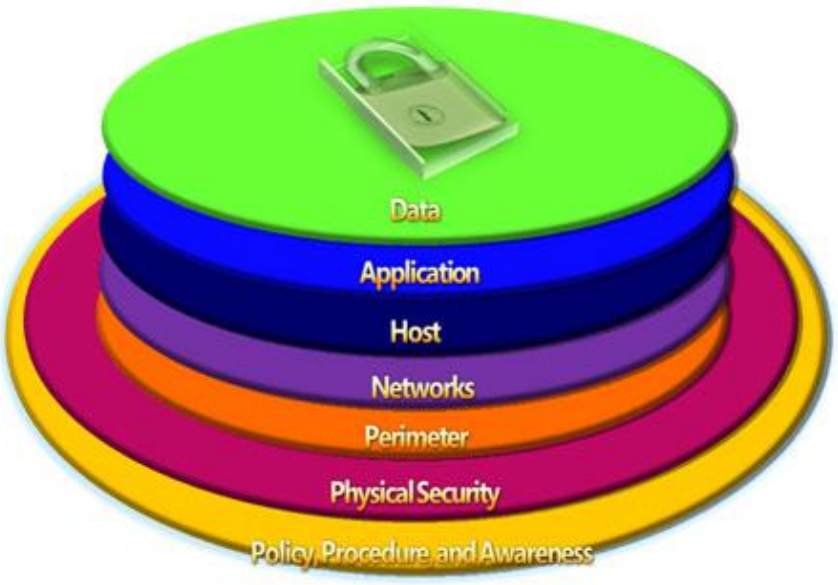
- Administración de parches. Mantener procedimientos de parcheo para asegurar actualización de software que ofrecen los fabricantes.

- Terminales de trabajo. Monitorearlas mediante herramientas como firewalls, antivirus y software de acceso remoto, controlando los cambios de software, hardware, servicios, otros.

Modelo de Defensa en Profundidad de Microsoft

El Modelo Seguridad en Profundidad, promovido por Microsoft como un conjunto necesario de prácticas para mantener seguro un sistema o una red de sistemas. Este modelo plantea la concepción de la seguridad como el efecto de una eficiente administración del riesgo, y propone una estructura definida en capas en las cuales se pueden implementar acciones estratégicas para asegurar cada una de éstas, y en el caso que alguna amenaza lograra filtrar la seguridad de alguna de estas capas, la siguiente capa, contara con sistemas de protección diferente y a otro nivel, logrando así mitigar los riesgos y evitar que el ataque pase a una siguiente etapa.

Imagen 1: Modelo en profundidad de Microsoft



Esta imagen simboliza con cada color cada una de las capas en las cuales se pueden definir estrategias acordes a la naturaleza de los posibles riesgos que hay en cada una de ellas. Existen muchas maneras de asegurar un nivel individualmente, dependiendo cual sea y sus particularidades, se utilizan tecnologías diferentes, o estrategias que apliquen para cada uno.

Acciones a Ejecutar en cada Capa:

Es importante mencionar, que cada acción de protección tiene un costo, por lo que en cada caso en particular debe evaluarse el valor de la información a proteger y los costos que implicaría la pérdida o el sufrimiento de un ataque, y en este sentido planificar las acciones pertinentes para la protección de tal información.

Seguidamente, se listan las acciones o estrategias que podrían aplicarse en cada una de las capas (Microsoft Virtual Academy. 2011):

- En primer lugar se encuentran los Procedimientos y Políticas de seguridad propias de la organización. Éstas se apoyan en estándares establecidos y programas educativos de seguridad para los usuarios
- La seguridad física es un elemento fundamental en una estrategia de seguridad global, abarcando las ubicaciones de los servidores, el acceso a los edificios de la organización, entre otros, con el fin de evitar ataques como la denegación de servicio, robo de datos, ejecución de código malicioso, y cualquier otro relacionado. Dentro de la seguridad física también se deben tener en cuenta la protección ante desastres naturales y ataques terroristas.
- Defensa de Perímetros lógicos: es el aspecto más importante para detener los ataques externos, así que se debe contar con algún dispositivo de seguridad para proteger cada punto de acceso a la red, evaluando el tipo de tráfico a permitir. Son útiles los servidores de seguridad con su correspondiente administración y auditoría con el fin de detectar intrusiones y evitar ataques a tiempo. Adicionalmente, si se requiere habilitar el acceso remoto a la red, los equipos cliente también deben cumplir con determinados requisitos de seguridad antes de conectarse remotamente.
- Defensa de Redes: si un enrutador sufre un ataque exitoso, puede denegar el servicio a segmentos o a toda una red, de tal forma que se

debe examinar el tráfico permitido en las redes existentes y bloquear el que no es necesario.

- Defensa de Hosts: se debe evaluar cada host del entorno y crear directivas que limiten las tareas que tenga que realizar, por ejemplo, creando directivas individuales en función de la clasificación y el tipo de datos que contiene cada servidor.

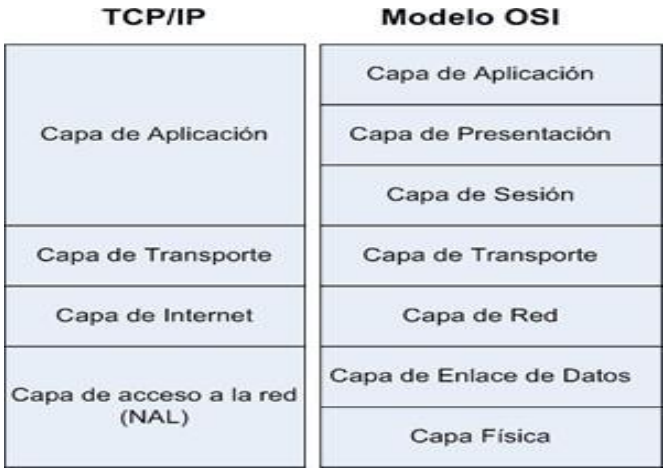
- Defensa de Aplicaciones: es responsabilidad del programador incorporar la seguridad en las aplicaciones para proporcionar una contramedida adicional. Debe existir un entorno de pruebas antes de ejecutar una configuración de producción. Todo esto, manteniendo protección de acceso y ejecución de dicho software.

- Defensa de Datos: los datos almacenados localmente en equipos de usuarios son especialmente vulnerables ante la ejecución de copias de seguridad, restaurar y leer los datos en otro equipo, aunque el delincuente no se conecte al sistema. Por lo tanto, los datos deben protegerse de alguna manera, por ejemplo, usando técnicas de cifrado de datos de fabricantes y la modificación de las listas de control de acceso a los archivos.

Modelos OSI Y TCP/IP

Siendo los modelos OSI y TCP/IP marcos de referencia para la definición de arquitecturas de Interconexión de Sistemas de comunicaciones, es necesario tenerlos en cuenta en el estudio de la seguridad en profundidad, en donde interactúan los protocolos, servicios, aplicaciones, dispositivos, políticas, personas, entre otros.

Imagen 2: Correspondencia de capas entre el modelo TCP/IP y OSI



Fuente; Corletti 2017

- Capa de Acceso a la red.

Se debe auditar el canal de comunicaciones que se emplee, el cual puede ser cable, fibra láser, radiofrecuencia, entre otros. Así mismo, se debe tener en cuenta:

- Identificación de los canales.
- Tramos críticos.
- Ubicación, acceso y componentes de los racks de comunicaciones.
- Planos e identificación completa del cableado estructurado.
- Documentación y control de cambios.
- Inventario actualizado de equipamiento.
- Almacenamiento de documentación y archivos como plan de resguardo.
- Restringir el acceso al centro de datos.
- Mecanismos de Backup para garantizar un resguardo a la información.
- Análisis de la topología de la red.
- Estrategias de expansión.
- Asignación de prioridades y reservas para el acceso a la red.
- Establecimiento de Redes privadas Virtuales.
- Aspectos eléctricos u ópticos.

Las herramientas que operan a este nivel son analizadoras de protocolos como:

-Control de direcciones de hardware.

-Auditoría de configuración de Switches.

-Análisis de tráfico el cual puede ser Unicast, Multicast, o Broadcast, afectando el rendimiento de la red.

-Análisis de colisiones con el fin de evitar un ataque de negación de servicio.

-Detección de Sniffers en la red.

-Monitorear los puntos de acceso inalámbrico.

- Capa de Internet.

Para TCP/IP existirá gran actividad en la red, por lo tanto se debe tener especial cuidado y monitoreo, a través de:

-Auditoría en Router: Control de contraseñas, configuración del router, backup de las configuraciones, protocolos de enrutamiento (RIP, IGRP, EIGRP, OSPF), listas de control de acceso, logs de eventos, seguridad en el acceso por consola.

- Auditoría de tráfico ICMP: Mejor ruta, solicitud y respuesta de eco (Ping), destino no alcanzable.

- Auditoría ARP: Analizar todas las tramas que circulan por la red y comparar permanentemente las mismas con un patrón de referencia.

- Auditoría de direccionamiento IP: Estático ó Dinámico.

- Detección de ataques.

- Capa de transporte.

Evaluar y monitorear los modos de conexión existentes.

- Auditoría de establecimientos y cierres de sesión.

- Auditoría en UDP: Cerrar todos los puertos UDP no utilizados.

- Auditoría en Puertos UDP y TCP.

- Auditoría de Troyanos.

- Capa de Aplicación.

Al estar directamente en contacto con el usuario, es una capa bastante especial, en donde la auditoría requiere gran atención, sin ser más importante que las capas anteriores, ya que puede verse afectada por suplantación y mal uso cuando no existen políticas adecuadas y correctamente difundidas entre el personal de la compañía.

- Auditoría de servidores de correo, Web, FTP y Proxy, vigilando su flujo de datos y establecimiento de sesiones.
- Auditoría de accesos remotos.
- Auditoría en Firewall.
- Bombardeos de mail.
- Auditoría en Servidores DNS.
- Auditoría en Servidores de correo.
- Auditoría en Servidores de archivos.

Existe gran variedad de tecnologías y protocolos de red que participan en cada capa del Modelo OSI, adoptadas por los fabricantes, proporcionando no solo interoperabilidad, sino seguridad en los servicios ofrecidos. Dentro de éstos encontramos, por ejemplo, DNS, FTP, HTTP, SMTP, XML, SSL NetBIOS, TCP, UDP, IP, IPX, Ethernet, HDLC, WiFi, Fibra óptica, cable coaxial, entre otros (Corletti 2017).

Pruebas de penetración o Pentesting

El termino PenTest es como comúnmente se denomina a los "Test de penetración" o en inglés "Penetration Tests", es un procedimiento que se realiza a través de un conjunto de técnicas y métodos que simulan el ataque a un sistema, esto nos sirve para evaluar la seguridad de los sistemas informáticos, redes y aplicaciones (De León 2017). En otras palabras, es el procedimiento sistemático y metodológico que intenta mediante diversos

pasos recrear las acciones ofensivas de un atacante (del mismo modo en que éste las haría sobre un sistema informático) para lograr acceder a él, con el fin de descubrir y reparar problemas de seguridad.

Esta prueba puede realizarse a través de medios físicos utilizando hardware o mediante ingeniería social, existen herramientas de prueba de penetración que simplemente analizan un sistema, así como aquellas que realmente atacan el sistema para encontrar vulnerabilidades. Las pruebas de penetración permiten evaluar vulnerabilidades a través de la identificación de las debilidades, analizar y categorizar las debilidades explotables y prever recomendaciones en base a las prioridades de la organización, para reducir riesgos.

Tipos de PenTest

Las pruebas de penetración pueden buscar las vulnerabilidades en partes específicas o en la totalidad de los sistemas informáticos críticos de la organización. La información que se emplea la dispone la organización de forma pública y privada. El entorno de desarrollo de pruebas de penetración puede ser realizado desde lugares externos o dentro de las instalaciones de la organización con el fin de evaluar sus políticas y mecanismos de seguridad.

Las pruebas de intrusión pueden ser:

- Caja blanca: el pentester tiene conocimiento de toda la organización, conoce el funcionamiento del sistema, arquitectura de red, sistemas operativos, etc.

Este representa el mejor de los casos puesto que el atacante ya cuenta con información antes de acceder al sistema.

- Caja negra: el pentester no tiene conocimiento del sistema, suele contratarse una empresa externa para que realice el trabajo.

- Caja Gris: el pentester simula ser un empleado de la organización, se le da un usuario y clave de acceso a los sistemas con el objetivo de encontrar posibles problemas que pueden ser aprovechados por usuarios internos.

Fases del Pen test

- Planeación: el pentester y el cliente definen las metas y objetivos de la prueba, de modo que ambas partes estén de acuerdo y comprendan que se desea obtener.

- Reconocimiento: se analiza de forma preliminar la información disponible, esta información debe ser proporcionada y tiene que ser clara y completa.

- Descubrimiento: se realiza la recolección de datos mediante herramientas de análisis, el pentester determinará lo siguiente: rangos de direcciones IP, dirección física de la empresa, datos personales de la empresa: números de teléfonos, nombres del personal y cuentas de correo electrónico y demás información que el pentester considere.

- Evaluación: esta se centra en el análisis de los datos encontrados en fases anteriores para determinar mediante herramientas de scanning los puntos de vulnerabilidad que afectan al sistema evaluado.

- Intrusión: el pentester en esta etapa utiliza el conocimiento adquirido en etapas anteriores para lograr acceder al sistema y obtener información de la misma.

- Análisis: evalúa las vulnerabilidades encontradas en etapas anteriores para determinar riesgos potenciales que afecten a la empresa.

- Reporte: se prepara un informe detallado con todos los procedimientos generales realizados en las pruebas, seguido del análisis de las vulnerabilidades y riesgos, y sugerencias de seguridad futura.

Metodologías para realizar Pruebas de Penetración

"Para llevar a cabo pruebas de penetración se debe acompañar de una metodología que se acople a las necesidades de la organización" (De León, 2017), esta metodología debe emplear procedimientos y técnicas para alcanzar los objetivos deseados. A continuación, se describen metodologías utilizadas en pruebas de penetración:

OWASP: (Open Web Application Security Project) Es un proyecto de código abierto dedicado a identificar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es una organización sin fines de lucro que apoya y administra los proyectos e infraestructura de OWASP. Su enfoque es más para pruebas de penetración de caja negra, se compone de: Fase pasiva: en esta el tester entiende la lógica del sistema evaluado. Fase activa: el tester prueba todas las herramientas recomendadas por la metodología [14].

ISSAF ((Information Systems Security Assessment Framework) Los Sistemas de Información del Marco de Evaluación de Seguridad son una metodología estructurada para el análisis de seguridad en múltiples dominios y detalles específicos de la prueba o de las pruebas para cada uno de ellos. Su objetivo es proporcionar procedimientos muy detallados para la comprobación de sistemas de información que reflejen situaciones reales [14].

OSSTMM: Por sus siglas en inglés, Open Source Security Testing Methodology Manual, es un manual que combina ambición, estudio y años de experiencia de profesionales en el área de la seguridad. Las pruebas

individuales no son particularmente revolucionarios, pero la metodología en conjunto representa un estándar de referencia en el área de testeo de seguridad. Dicho manual es un estándar profesional para el testeo de seguridad en cualquier entorno, desde el exterior al interior. Como cualquier estándar profesional, incluye los lineamientos, la ética del Auditor de Seguridad, la legislación sobre el testeo de seguridad y un conjunto integral de test.(Gavilánez, 2016).

Tabla 2: Comparación de Metodologías Pentesting

ASPECTOS	ISSAF	OSSTMM	OWASP
Permite realizar pruebas y análisis de seguridad	Si	Si	Si
Establece requisitos previos para la evaluación	Si	No	Si
La metodología define un proceso detallado para la realización de pruebas	Si	Si	Si
Define áreas de alcance	Si	No	Si
Contiene plantillas para realizar las pruebas	Si	Si	Si
Detalla técnicas para cada prueba	Si	No	Si
Contiene ejemplos de pruebas y resultados	Si	No	Si
Recomienda herramientas para cada prueba	Si	No	Si
Presenta procesos de análisis y evaluación de riesgos	Si	Si	Si
Define dimensiones de seguridad a evaluar	No	Si	Si
Establece valores o niveles de evaluación de riesgos	Si	Si	Si
Enumera y clasifica las vulnerabilidades encontradas	Si	No	Si
Realiza estimación de impacto	Si	Si	Si
Genera reportes e informes	Si	No	Si
Presenta contramedidas y recomendaciones	Si	No	Si
Contiene referencias a documentación y enlaces externos	Si	No	Si

Fuente: .Gavilánez, 2016

Herramientas para realizar Pruebas de Penetración (Franco y Col. 2013)

- Wireshark: Es un analizador de protocolo de red que satisface los estándares de industrias e instituciones educativas de todo el mundo y, por lo tanto, es una opción preferible para la mayoría de los probadores de penetración para verificar la fortaleza de los sitios frente a ataques de seguridad. Admite cientos de protocolos y no es exclusivo de ningún sistema operativo en particular. La documentación adecuada sobre Wireshark está disponible, lo que ayuda a aprender rápidamente
- Nmap: Se usa para escanear en red. Puede encontrar dispositivos finales de redes conectadas, sus puertos abiertos, ejecutar servicios y puede construir un mapa de red. También se pueden encontrar versiones de sistemas operativos, servicios y dominios en ejecución. Esta información se puede usar en combinación con vulnerabilidades bien conocidas que se encuentran en bases de datos de acceso público.
- Maltego: Es una herramienta de tipo OSINT (inteligencia de fuente abierta), que representa un grupo de herramientas que utilizan fuentes de información disponibles públicamente. La herramienta usa listas de índices y bases de datos para buscar información relevante.
- Metasploit Framework: Es un proyecto de código abierto que proporciona la infraestructura, el contenido y las herramientas para realizar pruebas de penetración y una amplia auditoría de seguridad. Consta de múltiples componentes que trabajan en conjunto para proporcionarle una herramienta completa de prueba de penetración.
- Nexpose: Es una solución de gestión de vulnerabilidades que combina la evaluación de vulnerabilidades y controles, la validación de vulnerabilidades y la planificación de remediación.
- OpenVAS: Es un marco que contiene varios servicios y herramientas forjadas de Nessus, funciona en Linux y Microsoft Windows. Utiliza varios

escáneres para descubrir vulnerabilidades en servidores desde una máquina cliente.

- Acunetix: Es una herramienta comercial especializada en auditar aplicaciones web en busca de vulnerabilidades y fallos que puedan comprometer la integridad de la aplicación y la información que contiene. Ofrece una gran cantidad de características que permiten configurar la herramienta para que la precisión del análisis aumente y así, obtener resultados más fiables en su reporte.
- Owas Zap: Es una herramienta gratuita de análisis dinámico de vulnerabilidades. Forma parte del grupo de proyectos de la fundación OWASP y es ampliamente utilizado alrededor del mundo. Ofrece gran cantidad de documentación y soporte además permite realizar distintos tipos de análisis y ataques, permitiendo configurar perfiles específicos para ajustarlos a las características de las aplicaciones.

CAPITULO III
MARCO METODOLOGICO

Tipo de Investigación

Según Hurtado (2006)), la investigación documental se concreta exclusivamente en la recopilación de información en diversas fuentes. Indaga sobre un tema en documentos escritos u orales, en concordancia con esto la presente Investigación es de tipo documental ya que como su nombre lo indica se apoya en fuentes bibliográficas como libros, revistas, informes, tesis, entre otras.

Además, según el grado de profundidad es una investigación exploratoria, pues destaca los aspectos fundamentales de la Defensa en Profundidad en el ámbito organizacional, proporcionando los procedimientos adecuados para investigaciones posteriores.

En este orden de ideas, Fidias Arias (2010) la investigación exploratoria es aquella que se efectúa sobre un tema u objeto desconocido o poco estudiado, por lo que sus resultados constituyen una visión aproximada de dicho objeto.

Por su parte, Hernández, Fernández y Baptista (2012), opinan que los estudios exploratorios en pocas ocasiones constituyen un fin en sí mismos, por lo general determinan tendencias, identifican relaciones potenciales entre variables y establecen el tono de investigaciones posteriores más rigurosas.

Se caracterizan estos estudios, por ser más flexibles en su metodología en comparación con los estudios descriptivos o explicativos, y son más amplios y dispersos Su utilidad radica en familiarizarse sobre fenómenos nuevos o relativamente desconocidos y establecer prioridades para estudios futuros.

Etapas de la Investigación

- Selección del Tema de investigación: en este punto inicial el autor decidió inicialmente enfocarse en la seguridad informática pero al comenzar a recopilar la información se detectó que el titulo era un tema muy amplio y se necesitaba que fuera más específico y concreto, orientando el estudio específicamente en la defensa en profundidad.

  Así se definió el título, el objetivo general y los objetivos específicos que orientarían la investigación.

- Delimitación del Problema de investigación: la investigación se delimito espacial y temporalmente.

- Elaboración de una Guía de trabajo: inicialmente se elaboró un esquema de trabajo para tener un registro visual de las partes principales y subordinadas los temas clasificándolas en categorías o capítulos y subcapítulos, se analizó si había información suficiente y adecuada, chequeando lo que faltaba agregar, o eliminando textos superfluos para equilibrar la información. Fue necesario variar el esquema, según la experiencia adquirida con la información recolectada, siendo necesario buscar nuevas informaciones y realizar nuevos fichajes bibliográficos.

  - Recolección de la Información: Se realizó a través del fichero bibliográfico y de contenido. Se realizaron lecturas minuciosas de la bibliografía extrayendo las ideas más importantes que se registraron en las fichas de contenido, esto permitió la valoración del material recopilado, la localización de posibles lagunas, detección de excesos en las ideas transcritas, a fin de darle mayor organización y uniformidad a la investigación y para saber si faltan datos importantes.
  - Posteriormente se procedió a la clasificación pormenorizada de la información de acuerdo con los temas, categorías o capítulos y subcapítulos de la investigación que se elaboraron al principio.

Arias, F. (2006), expresa que “se entiende por técnicas, el procedimiento o forma particular de obtener datos o información”, estas informaciones se deben asentar o archivar en hojas de trabajo llamadas instrumentos que son para el citado autor medio y material que se emplean para recoger y almacenar la información. Para recabar la información necesaria y pertinente para el estudio se utilizan las siguientes técnicas e instrumentos

Técnicas e Instrumentos de Recolección de Datos.

El Cuestionario

Basado en lo que señalan Hernández y otros (2010): “el cuestionario consiste en un conjunto de ítems presentados en forma de afirmaciones o juicios entre los cuales se pide la reacción de los sujetos a los que se les administra”. Cuando se elabora un cuestionario se debe especificar sobre qué tema se recogen opiniones, a quien se le aplica y el tipo de información que se desea obtener. Las preguntas deben ser claras, precisas y adecuadas al nivel educativo de las personas que van a responder.

El cuestionario diseñado para el presente estudio por ser un cuestionario auto administrado se realizó de forma breve por lo cual solo constó de solo 6 items, con un escalamiento tipo Likert, contentiva de 3 opciones: Si, No, No sé/No respondo. Se utilizó una muestra intencional conformada por 27 empresas del sector servicios (bancos, salud, hoteles, entre otros), y 12 empresas del sector agroindustrial, para un total de 37 Pequeñas y Medianas Empresas (PyMEs) de la Ciudad de Valera, con la finalidad de obtener la información necesaria en relación al conocimiento sobre seguridad informática y su utilización por este tipo de empresas.

Técnica de Procesamiento y Análisis de Datos

En consideraciones de Hernández y otros (2010), el registro de los datos consiste en “el proceso que se realiza mediante un plan para clasificar los datos disponibles”. Por lo tanto para que la información recolectada tuviera significancia dentro de la presente investigación, y con el propósito de intentar dar respuesta al problema planteado, los datos obtenidos a través del cuestionario, fueron sometidos a un proceso de elaboración técnica, mediante la estadística descriptiva, considerando la frecuencia y el porcentaje de las respuestas dadas, lo que permitió recontarlos y resumirlos; antes de proceder a su análisis e interpretación.

CAPITULO IV
ANALISIS DE LOS RESULTADOS

Los datos se presentan tanto en tablas de frecuencias absolutas y porcentuales, como de manera gráfica, para representar la opinión emitida por los participantes. De la misma manera el análisis e interpretación de los datos se realizó atendiendo a las opciones de mayor frecuencia en las

respuestas, lo cual permite obtener una visión global y detallada de la situación.

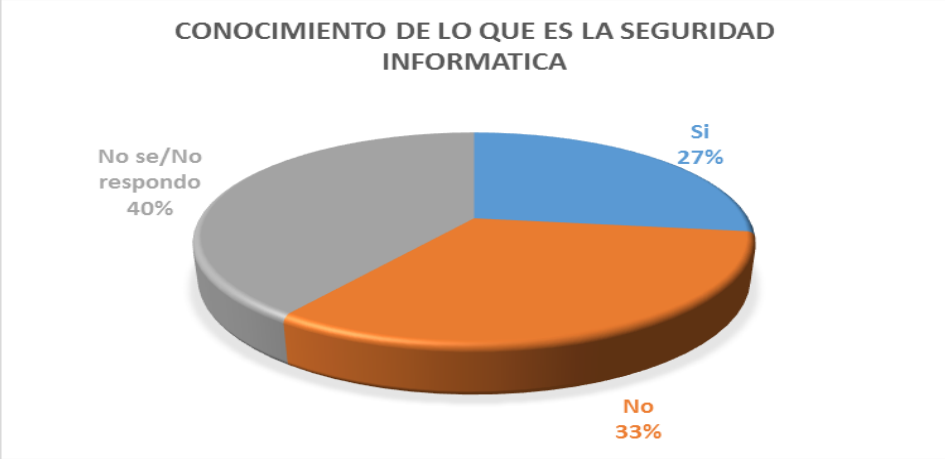
Ítem Nº 1: Tiene conocimiento de lo que es la seguridad informática?

Tabla Nro. 3: Distribución de frecuencia para el Item Nª1

ESCALA	F. ABSOLUTA	%
Si	10	27%
No	12	33%
No se/No respondo	15	40%
TOTAL	37	100%

Fuente: Rojo 2020

Grafico Nro. 3: Conocimiento de lo que es la seguridad informática



Como se puede observar en este grafico la mayoría de las empresas representadas en el 40% no respondieron, lo que es lógico en este tipo de encuestas auto administradas, seguido por un porcentaje discreto correspondiente al 27% que respondió que sí tienen conocimiento sobre seguridad informática, y hay que resaltar que el porcentaje que no tiene ni idea de lo que es la seguridad informática es significativo representado por un 33%, lo cual es negativo en términos generales.

Ítem Nº 2.: Cuenta su organización con una estrategia integral de seguridad para que su sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad?

Tabla Nro. 4: Distribución de frecuencia del ítem Nª 2

ESCALA	F. ABSOLUTA	%
Si	1	3%
No	21	57%
No se/No respondo	15	40%
TOTAL	37	100%

Fuente: Rojo 2020

Grafico Nª 2; La Empresa cuenta con alguna estrategia integral se seguridad

En este grafico se evidencia que el 43% de los encuestados, no cuenta con sistemas de seguridad informatica que les permita mantener la informacion segura. Esto según corvetti (2017), es una desventaja muy peligrosa para las organizaciones de cualquier tipo.

Ítem Nº 3: Ha sido víctima su empresa de alguna violación a su seguridad informática?

Tabla Nª 5: Distribución de frecuencia del ítems Nª 3

ESCALA	F. ABSOLUTA	%
Si	22	60%
No	0	0%
No se/No respondo	15	40%
TOTAL	37	100%

Fuente: Rojo 2020

Grafico Nª 3: Violación a la seguridad informática

La totalidad de las empresas encuestadas expresan que han sufrido alguna infracción a su seguridad informática, esto está en concordancia con lo expresado en el informe sobre Seguridad Cibernética de la Organización de Estados Americanos (OEA, 2014), que indica que en los últimos años se ha incrementado los ciberataques a las compañías, especialmente a las PyMEs. Estas son un claro objetivo de los hacker ya que disponen de menos recursos para protegerse.

Item Nª 4: Conoce su organización lo que es la defensa en profundidad?

Tabla Nro. 6: Distribución de frecuencia del ítem Nª 4

ESCALA	F. ABSOLUTA	%
Si	0	60%
No	22	0%
No se/No respondo	15	40%
TOTAL	37	100%

Fuente: Rojo 2020

Grafico Nª 4 : Conocimiento de la Defensa en Profundidad

Aquí se puede evidenciar que existe un desconocimiento general del tema de la defensa en profundidad por parte de las PyMEs, en la ciudad de Valera, como lo indica el hecho que el 60% de los encuestados que son la totalidad de las empresas que respondieron la encuesta dijeron que no saben lo que significa en término. Esto representa una debilidad de acuerdo a lo mencionado por corvetti (2017).

Ítem Nº 5: Tiene algún conocimiento de lo que son las pruebas de penetración o pentesting?

Tabla Nro. 7: Distribución de frecuencia del ítem Nª 5

ESCALA	F. ABSOLUTA	%
Si	0	60%
No	22	0%
No se/No respondo	15	40%
TOTAL	37	100%

Fuente: Rojo 2020

Grafico Nª 5 : Conocimiento del Pentesting

Del mismo modo que en el ítem anterior, se observa que todas las empresas que respondieron la encuesta expresan su desconocimiento en el tema referido al pentesting, lo cual también se constituye en una desventaja para las PyMEs en Valera.

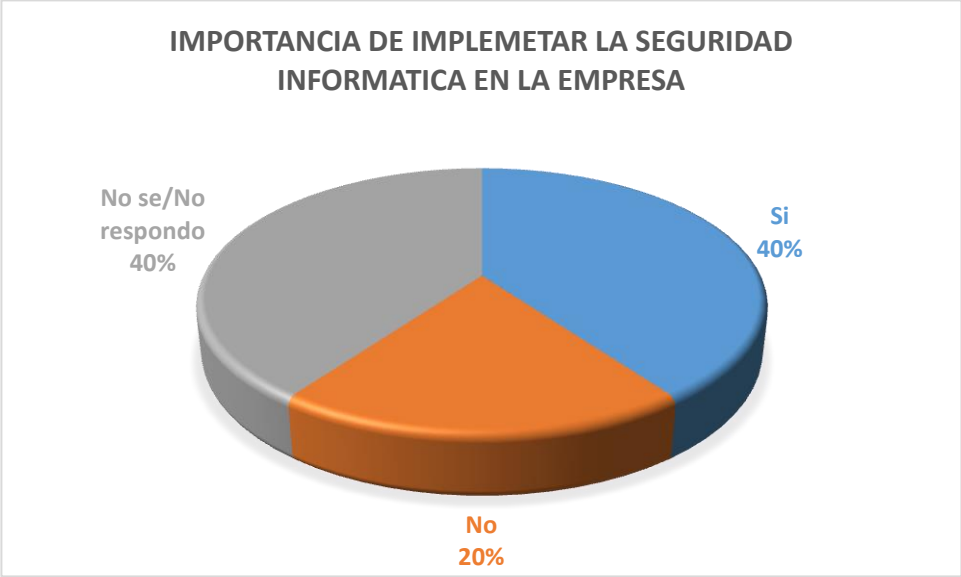
Ítem Nº 6: Considera Importante implementar alguna procedimiento de seguridad informática en su empresa?

Tabla Nª 8. Distribución de frecuencia del ítem Nª 6

ESCALA	F. ABSOLUTA	%
Si	15	40%
No	7	20%
No se/No respondo	15	40%
TOTAL	37	100%

Fuente: Rojo 2020

Grafico Nª 5: Importancia de implementar la seguridad informática en la empresa



En este grafico se observa, que el 40% de las PyMEs consideran importante la implementacion de la seguridad informatica en sus empresas, esto es un indicador de que la ciberseguridad ha comenzado a ganarse un lugar importante en el medio empresarial, por lo que la protección en torno a todo lo que tiene que ver con Internet y sus libertades es un tema delicado para muchas empresas.

CONCLUSIONES

Una vez que estuvo recopilada, tabulada y analizada la información obtenida del instrumento que se aplicó, en consecuencia, se procede a generar las conclusiones derivadas del proceso de investigación que se llevó a cabo, en torno a Describir el modelo de Defensa en Profundidad y el

Pentesting como técnicas de seguridad informática. Las conclusiones se realizan en concordancia con cada uno de los objetivos específicos formulados y al final con un comentario sobre los resultados obtenidos, respecto al objetivo general de la investigación

En cuanto al primer objetivo que consiste en: Describir los procedimientos de Seguridad informática, especialmente lo referente a la Defensa en Profundidad, fue posible materializarlo a través de la revisión exhaustiva del material bibliográfico que permitió puntualizar estos procedimientos y temas referentes a la ciberseguridad, como lo expresa Aguilera (2011), cuando dice que se puede definir a la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad. y se concluye que las ciberamenzas siempre estarán presentes y prestas a atacar un sistema de información, esta afirmación se fundamenta en lo

En relación al segundo objetivo orientado a: Caracterizar el pentesting, como método de evaluación integral y detección temprana de fallas de seguridad en los sistemas informáticos, se pudo conocer que es un procedimiento comúnmente utilizado y efectivo para la detección de fallos de seguridad informática

Esta conclusión se fundamenta en lo expresado De León (2017), cuando señala que el pentesting es el procedimiento sistemático y metodológico que intenta mediante diversos pasos recrear las acciones ofensivas de un atacante (del mismo modo en que éste las haría sobre un sistema informático) para lograr acceder a él, con el fin de descubrir y reparar problemas de seguridad.

En definitiva, se puede señalar que el penstesting y la defensa en profundidad son técnicas, que al aplicarse de manera conjunta pueden garantizar un buen nivel de seguridad dentro de los un sistemas de información

Por otra parte, el tercer objetivo enfocado en Diagnosticar la situación actual referente a la Seguridad Informática en las Pequeñas y Medianas Empresas en la Ciudad de Valera, Estado Trujillo, se pudo precisar que las PyMEs, aunque en su mayoría han experimentado algún problema relacionado con la seguridad informática, no conocen ni aplican metodologías de seguridad que les permita proteger su información vital.

Es importante señalar, que un porcentaje significativo representado por el 40% de las empresas encuestadas, no respondieron, lo que es lógico en este tipo de encuestas auto administradas.

Ahora bien, en relación al Objetivo General, se considera que fue logrado en su totalidad, tal como lo evidencia todo el análisis y la discusión de cada uno de los objetivos específicos alcanzados, y además por la comúnmente conocida premisa metodológica de que, “el alcance de los objetivos específicos implica el alcance del objetivo general”.

RECOMENDACIONES

Después de haber presentado las conclusiones del estudio, corresponde sugerir la realización de algunas actividades como consecuencia de la acción investigativa desarrollada, dirigidas a solventar las deficiencias que se pudieron evidenciar. Estas orientaciones son:

Dar a conocer los resultados de la presente investigación a las Pequeñas y Medianas Empresas del estado Trujillo, y especialmente a las de la ciudad de Valera, tanto del sector industrial como del de servicios. Esta acción se realizaría con el propósito de difundir el conocimiento pertinente a sus organizaciones que conlleva el estudio, y que éstas tomen conciencia de la importancia de la seguridad informática para sus organizaciones.

Así mismo, se sugiere la socialización del producto de la presente investigación a los alumnos de la carrera de Ingeniería de Computación en la Universidad Valle del Momboy, para que se interesen en realizar más Trabajos de Investigación en el área de la seguridad informática.

REFERENCIAS BIBLIOGRAFICAS

Arias, F. (2006). El Proyecto de Investigación (Introducción a la Metodología Científica). Caracas: Episteme.

Cisco. (2018). cisco. Obtenido de cisco: Disponible en: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html (consultado el 15 de octubre de 2019)

Corletti Alejandro. Ciberseguridad. 2017. Madrid

De León Velásquez, "Test de penetración 'pentesting' aplicado en entornos gnu/linux en una empresa Guatemalteca," Universidad Mariano Gálvez de Guatemala Facultad de Ingeniería en Sistemas de Información y Ciencias de la Computación, 2017.

Dussan, C., "Políticas de seguridad informática," Entramado, vol. 2, no. 1, pp. 86–92, 2006.

Franco, D., Perea J., y Tovar L., "Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios," vol. 24, no. 5, pp. 13–22, 2013

Hernández, Roberto; Fernández, Carlos; y Baptista, Pilar (2012). Metodología de la Investigación. México: Mc Graw-Hill.

Hurtado de Barrera, J. (2006). El proyecto de investigación. Bogotá: Quirón

Larraz, T. (2010). "Spanish "botnet" potent enough to attack country: police", en Reuters. Disponible en: https://www.reuters.com/article/us-crimehackers/spanish-botnet-potent-enough-to-attack-country-policeid (Consultado el 10 de diciembre de 2019).

Ríos R., Reyes J., Morales L., Sandoya D., y Miranda M., "Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas," Rev. Publicando, vol. 10, pp. 462–473, 2017.

Saint-Pierre, H. (2012), “Fundamentos para pensar la distinción entre defensa
y seguridad”, en RESDAL (Ed.). Atlas comparativo de la Defensa en América Latina y el Caribe. Buenos Aires: RESDAL.

Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information. (consultado el 02 de noviembre 2019). “La defensa en profundidad aplicada a los sistemas de información”. Disponible: https://www.ssi.gouv.fr/archive/es/confianza/documents/methods/mementodep-V1.1_es.pdf.